

1 Frank S. Hedin (SBN 291289)
Hedin LLP
2 535 Mission Street, 14th Floor
3 San Francisco, CA 94105
Telephone: (305) 357-2107
4 Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com
5

6 *Attorney for Plaintiff and the Putative Class*

7 **UNITED STATES DISTRICT COURT**
8 **FOR THE EASTERN DISTRICT OF CALIFORNIA**

9 JENNIFER CARRUTH, individually and on behalf
of all others similarly situated,

10 Plaintiff,

11 v.

12 KD CREATIVES, INC. D/B/A BIG LITTLE
13 FEELINGS,

14 Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

15 Plaintiff JENNIFER CARRUTH, individually and on behalf of all others similarly situated,
16 makes the following allegations pursuant to the investigation of counsel and based upon information
17 and belief, except as to allegations pertaining specifically to herself or her counsel, which are based
18 on personal knowledge.

19 **NATURE OF THE CASE**

20
21 1. Plaintiff brings this action for legal and equitable remedies to redress and put a stop to
22 Defendant KD CREATIVES, INC. d/b/a BIG LITTLE FEELINGS' practices of knowingly selling,
23 transmitting, and/or otherwise disclosing, to various third parties, records containing the personal
24 information (including names and addresses) of each of their purchasers (collectively "Personal
25 Viewing Information") in violation of the Video Privacy Protection Act, 18 U.S.C. §2710 et. seq.
26 ("VPPA").
27
28

1 2. Over the past two years, Defendant has systematically transmitted (and continues to
2 transmit today) its purchasers' personally identifying video viewing information to Meta using a
3 snippet of programming code called the "Meta Pixel," which Defendant chose to install on its
4 biglittlefeelings.com website.

5 3. The information Defendant disclosed (and continues to disclose) to Meta, via the
6 Meta Pixel it installed on its website, includes a consumer's Facebook ID ("FID") coupled with their
7 purchase and the title of each of the specific videos that the consumer requested or obtained on
8 Defendant's website. A purchaser's FID is a unique sequence of numbers linked to the Meta profile
9 belonging to that purchaser. The purchaser's Meta profile, in turn, publicly identifies the purchaser
10 by name (and contains other personally identifying information about the purchaser as well).
11 Entering "facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom
12 the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous
13 persons may share the same name but each person's Facebook profile (and associated FID) uniquely
14 identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant
15 captures and discloses to Meta information that reveals the specific videos that a particular person
16 viewed as a purchaser of Defendant's website (hereinafter, "Private Viewing Information").
17

18 4. Defendant disclosed and continues to disclose that a consumer purchased a
19 subscription to Defendant's website and its purchasers' Private Viewing Information to Meta
20 without asking for let alone obtaining its purchasers' consent to these practices.
21

22 5. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the
23 VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service
24 provider who knowingly discloses, to any person, personally identifiable information concerning
25 any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1),
26
27
28

1 *inter alia*, liquidated damages in the amount of \$2,500.00 per violation and equitable relief, *see id.*
2 § 2710(c).

3 6. Accordingly, on behalf of herself and the putative Class members defined below,
4 Plaintiff brings this Class Action Complaint against Defendant for intentionally and unlawfully
5 disclosing their Personal Viewing Information to Meta.
6

7 **PARTIES**

8 **I. Plaintiff**
9

10 7. Plaintiff is, and at all times relevant hereto was, a citizen and resident of San Diego
11 County, California.

12 8. Plaintiff is, and at all times relevant hereto was, a user of Meta.
13

14 9. On or about January 10, 2023, Plaintiff purchased prerecorded video material from
15 Defendant by requesting and paying for such material on Defendant's website, and by providing her
16 name, email address, and home address. Accordingly, Plaintiff requested or obtained, and is therefore
17 a consumer of, prerecorded video material sold by Defendant on its website.

18 10. At all times relevant hereto, including when purchasing prerecorded video material
19 from Defendant on its website, Plaintiff had a Meta account, a Meta profile, and an FID associated
20 with such profile.
21

22 11. When Plaintiff purchased prerecorded video material from Defendant on its website,
23 Defendant disclosed to Meta Plaintiff's FID coupled with the specific title of the video she purchased
24 (as well as the URL where such video is available for purchase), among other information concerning
25 Plaintiff and the device on which she used to make the purchase.

26 12. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to
27 disclose her Personal Viewing Information to Meta. In fact, Defendant never even provided Plaintiff
28

1 with written notice of its practices of disclosing its customers' Personal Viewing Information to third
2 parties such as Meta.

3 13. Because Defendant disclosed Plaintiff Private Viewing Information (including her
4 FID, the title of the prerecorded video material she purchased from Defendant's website, and the URL
5 where such video is available for purchase) to Meta during the applicable statutory period, Defendant
6 violated Plaintiff's rights under the VPPA and invaded her statutorily conferred interest in keeping
7 such information (which bears on her personal affairs and concerns) private.
8

9 **II. Defendant KD Creatives, Inc. d/b/a Big Little Feelings**

10 14. Defendant is a California Corporation with its office located at 7801 Folsom Blvd.
11 #202, Sacramento, CA 95826.
12

13 15. Defendant operates and maintains the website biglittlefeelings.com, where it sells pre-
14 recorded video courses to consumers across the country.

15 **JURISDICTION AND VENUE**

16 16. This Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C.
17 § 1331 and 18 U.S.C. § 2710.

18 17. Personal jurisdiction and venue are proper because Defendant conducts business and
19 streams the prerecorded videos it sells to a considerable number of consumers, such as Plaintiff,
20 within this judicial District.
21

22 **VIDEO PRIVACY PROTECTION ACT**

23 18. Generally speaking, the VPPA prohibits companies like Defendant from knowingly
24 disclosing to third parties like Facebook information that personally identifies consumers like Plaintiff
25 as having viewed particular videos or other audio-visual products or services.

26 19. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits
27 "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable
28

1 information concerning any consumer of such provider[.]” 18 U.S.C. § 2710(b)(1). The statute defines
2 a “video tape service provider” as “any person, engaged in the business...of rental, sale, or delivery
3 of prerecorded video cassette tapes or similar audio visual materials,” 18 U.S.C. § 2710(a)(4), and
4 defines a “consumer” as “a renter, purchaser, or purchaser of goods or services from a video tape
5 service provider.” 18 U.S.C. § 2710(a)(1). “[P]ersonally identifiable information” includes
6 information which identifies a person as having requested or obtained specific video materials or
7 services from a video tape service provider.” 18 U.S.C. § 2710(a)(3)

9 20. The VPPA’s purpose is as apropos today as it was at the time of its enactment over 35
10 years ago. Leading up to the statute’s enactment in 1988, members of the United States Senate
11 warned that “[e]very day Americans are forced to provide to businesses and others personal
12 information without having any control over where that information goes.” *Id.* Senators at the time
13 were particularly troubled by disclosures of records that reveal consumers’ purchases and rentals of
14 videos and other audiovisual materials, because such records offer “a window into our loves, likes,
15 and dislikes,” such that “the trail of information generated by every transaction that is now recorded
16 and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of
17 surveillance.” S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy,
18 respectively).

20
21 21. Thus, in proposing the Video and Library Privacy Protection Act (which later became
22 the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to
23 codify, as a matter of law, that “our right to privacy protects the choice of movies that we watch with
24 our family in our own homes.” 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained
25 at the time, it is the personal nature of such information, and the need to protect it from disclosure,
26 that is the *raison d’être* of the statute: “These activities are at the core of any definition of personhood.
27 They reveal our likes and dislikes, our interests and our whims. They say a great deal about our
28

1 dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us
2 as people.” *Id.*

3 22. While these statements rang true in 1988 when the act was passed, the importance of
4 legislation like the VPPA in the modern era of data mining is more pronounced than ever before.
5 During a recent Senate Judiciary Committee meeting, “The Video Privacy Protection Act: Protecting
6 Viewer Privacy in the 21st Century,” Senator Leahy emphasized the point by stating: “While it is true
7 that technology has changed over the years, we must stay faithful to our fundamental right to privacy
8 and freedom. Today, social networking, video streaming, the ‘cloud,’ mobile apps and other new
9 technologies have revolutionized the availability of Americans’ information.”¹

10
11 23. Former Senator Al Franken may have said it best: “If someone wants to share what
12 they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right
13 to easily control who finds out what they watch—and who doesn’t. The Video Privacy Protection Act
14 guarantees them that right.”²

15
16 24. In this case, however, Defendant deprived Plaintiff and the unnamed Class members
17 of that right by systematically (and surreptitiously) disclosing their Personal Viewing Information to
18 Facebook, without providing notice to (let alone obtaining consent from) any of them, as explained
19 in detail below.
20
21
22
23
24

25 ¹ The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee
26 Subcommittee on Privacy, Technology and the Law, <http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury>.

27 ² Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century,
28 frank.senate.gov (Jan. 31, 2012).

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

25. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."³

26. More than a decade later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a \$26 billion dollar per year online advertising industry in the United States.⁴

27. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.⁵

28. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.⁶

³ FCC, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

⁴ See *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html>.

⁵ Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

⁶ See M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), <http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/>.

29. The scope of data aggregators’ knowledge about consumers is immense: “If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on.”⁷

30. Further, “[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available.”⁸

31. Recognizing the serious threat the data mining industry poses to consumers’ privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.⁹

32. Data aggregation is especially troublesome when consumer information is sold to direct-mail

33. Disclosures like Defendant’s are particularly dangerous to the elderly. “Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on

⁷ N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at <http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html>.

⁸ Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012), available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c.

⁹ See *Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers’ Personal Information*, Website of Sen. Markey (July 24, 2012), <http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information>.

1 delivery services, and are lonely for the companionship that telephone callers provide.”¹⁰ The FTC
 2 notes that “[t]he elderly often are the deliberate targets of fraudulent telemarketers who take
 3 advantage of the fact that many older people have cash reserves or other assets to spend on seemingly
 4 attractive offers.”¹¹

5
 6 34. Indeed, an entire black market exists while the personal information of vulnerable
 7 elderly Americans is exchanged. Thus, information disclosures like Defendant’s are particularly
 8 troublesome because of their cascading nature: “Once marked as receptive to [a specific] type of
 9 spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists.”¹²

10 35. Defendant is not alone in violating its customers’ statutory rights and jeopardizing
 11 their well-being in exchange for increased revenue: disclosing customer and purchaser information
 12 to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has
 13 become a widespread practice. Unfortunately for consumers, however, this growth has come at the
 14 expense of their most basic privacy rights.
 15

16 **II. Consumers Place Monetary Value on their Privacy and Consider Privacy Practices** 17 **When Making Purchases**

18 36. As the data aggregation industry has grown, so too have consumer concerns regarding
 19 their personal information.

20 37. A recent survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed
 21 that 89 percent of consumers polled avoid doing business with companies who they believe do not
 22
 23
 24

25 ¹⁰ *Id.*

26 ¹¹ *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging* (August 10, 2000) (prepared
 27 statement of the FTC), available at https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf.

28 ¹² *Id.*

1 protect their privacy online.¹³ As a result, 81 percent of smartphone users polled said that they avoid
2 using smartphone apps that they don't believe protect their privacy online.¹⁴

3 38. Thus, as consumer privacy concerns grow, consumers are increasingly incorporating
4 privacy concerns and values into their purchasing decisions and companies viewed as having weaker
5 privacy protections are forced to offer greater value elsewhere (through better quality and/or lower
6 prices) than their privacy- protective competitors.

7 39. In fact, consumers' personal information has become such a valuable commodity that
8 companies are beginning to offer individuals the opportunity to sell their personal information
9 themselves.¹⁵

10 40. These companies' business models capitalize on a fundamental tenet underlying the
11 personal information marketplace: consumers recognize the economic value of their private data.
12 Research shows that consumers are willing to pay a premium to purchase services from companies
13 that adhere to more stringent policies of protecting their personal data.¹⁶

14 41. Thus, in today's digital economy, individuals and businesses alike place a real,
15 quantifiable value on consumer data and corresponding privacy rights.¹⁷ As such, where a business
16

17
18
19 ¹³ See 2014 TRUSTe US Consumer Confidence Privacy Report, TRUSTe, [http://www.theagitator.net/wp-](http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf)
20 [content/uploads/012714_ConsumerConfidenceReport_US1.pdf](http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf).

21 ¹⁴ *Id.*

22 ¹⁵ See Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12,
23 2012), available at [http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-](http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html)
24 [personal-data.html](http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html).

25 ¹⁶ See Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*,
26 22(2) Information Systems Research 254, 254 (2011); see also European Network and Information Security Agency,
27 *Study on monetising privacy* (Feb. 27, 2012), available at [https://www.enisa.europa.eu/activities/identity-and-](https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy)
28 [trust/library/deliverables/monetising-privacy](https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy).

¹⁷ See Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available
at <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf> ("It is obvious that people
value online privacy.").

1 offers customers a service that includes statutorily guaranteed privacy protections, yet fails to honor
2 these guarantees, the customer receives a service of less value than the service paid for.

3 **III. Defendant Systematically Discloses its Purchasers' Personal Viewing Information to**
4 **Meta**

5 42. As alleged below, whenever a person with a Meta account purchases prerecorded
6 video material from Defendant on its website, the Meta Pixel technology that Defendant intentionally
7 installed on its website transmits the customer's personally identifying information and detailed
8 Private Viewing Information (revealing the specific titles of the prerecorded video material that he or
9 she purchased) to Meta – all without the customer's consent, and in clear violation of the VPPA.
10

11 **A. The Meta Pixel**

12 43. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known
13 as "Meta".¹⁸ Since then, Meta has become the world's largest social media platform. To create a Meta
14 account, a person must provide, *inter alia*, her or her first and last name, birthdate, gender, and phone
15 number or email.
16

17 44. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of
18 code that companies can embed on their websites to allow them to track consumers' actions and
19 report the actions back to Meta.

20 45. The Meta Pixel allows online-based companies like Defendant to build detailed
21 profiles about their visitors by collecting information about how they interact with their websites, and
22 to then use the collected information to service highly targeted advertising to them.

23 46. Additionally, a Meta Pixel installed on a company's website allows Meta "to match .
24 . . website visitors to their respective [Meta] User accounts."¹⁹ Meta is able to do this because it has
25

26
27 ¹⁸ Company Info, FACEBOOK, <https://about.fb.com/company-info/>.

28 ¹⁹ <https://developers.facebook.com/docs/meta-pixel/get-started>.

1 assigned to each of its users an “FID” number – a unique and persistent identifier that allows anyone
2 to look up the user’s unique Meta profile and thus identify the user by name²⁰ – and because each
3 transmission of information made from a company’s website to Meta via the Meta Pixel is
4 accompanied by, *inter alia*, the FID of the website’s visitor. Moreover, the Meta Pixel can follow a
5 consumer to different websites and across the Internet even after clearing browser history.
6

7 47. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised
8 of highly detailed personally identifying information about each of its billions of users worldwide,
9 including information about all of its users’ interactions with any of the millions of websites across
10 the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by
11 selling advertisers the ability to serve highly targeted advertisements to the persons whose personal
12 information is contained within it.
13

14 48. Simply put: if a company chooses to install the Meta Pixel on its website, both the
15 company who installed it and Meta (the recipient of the information it transmits) are then able to
16 “track[] the people and type of actions they take”²¹ on the company’s website, including the purchases
17 they made, the items they spent time viewing, and, as relevant here, the specific video content that
18 they requested or obtained on the website.
19

20 **B. Defendant Knowingly Uses the Meta Pixel to Transmit the Private Viewing
21 Information of all of its Customers to Meta**

22 49. Defendant sells a wide variety of prerecorded video materials, including parenting
23 courses, to consumers on its website www.biglittlefeelings.com.
24

25 50. To make a purchase of prerecorded video material from Defendant’s website, a person
26

27 ²⁰ For example, Mark Zuckerberg’s FID is reportedly the number “4,” so logging into Facebook and typing
28 www.facebook.com/4 in the web browser retrieves Mark Zuckerberg’s Facebook page: www.facebook.com/zuck, and
all of the additional personally identifiable information contained therein.

²¹ <https://www.facebook.com/business/goals/retargeting>.

1 must provide at least his or her name, email address, billing address, and credit or debit card (or other
2 form of payment) information.

3 51. Whenever a person with a Meta account purchases prerecorded video material from
4 Defendant on its website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel
5 to disclose to Meta the unencrypted FID of the person who made the purchase and the specific title
6 of video material that the person purchased (as well as the URL where such video material is available
7 for purchase).

9 52. In order to take advantage of the targeted advertising and other informational and
10 analytical services offered by Meta, Defendant intentionally programmed its website (by following
11 step-by-step instructions from Meta’s website) to include the Meta Pixel code, which systematically
12 transmits to Meta the FID of each person with a Meta account who purchases prerecorded video
13 material on its website, along with the specific title of the prerecorded video material that the person
14 purchased.

16 53. With only a person’s FID and the title of the prerecorded video material (or URL
17 where such material is available for purchase) that the person purchased from Defendant on its
18 website—all of which Defendant knowingly provides to Meta on a systematic basis—any ordinary
19 person could learn the identity of the person to whom the FID corresponds and the title of the specific
20 prerecorded video material that the person purchased (and thus requested and obtained). This can be
21 accomplished simply by accessing the URL [www.facebook.com/\[insert the person’s FID here\]/](http://www.facebook.com/[insert the person’s FID here]/).

23 54. Defendant’s practices of disclosing the Private Viewing Information of its customers
24 to Meta continued unabated for the duration of the two-year period preceding the filing of this action.
25 At all times relevant hereto, whenever Plaintiff or any other person purchased prerecorded video
26 material from Defendant on its website, Defendant disclosed to Meta (*inter alia*) the specific title of
27 the video material that was purchased (including the URL where such material is available for
28

1 purchase), along with the FID of the person who purchased it (which, as discussed above, uniquely
2 identified the person).

3 55. At all times relevant hereto, Defendant knew that the Meta Pixel was disclosing its
4 customers' Private Viewing Information to Meta.

5 56. Although Defendant could easily have programmed its website so that none of its
6 customers' Private Viewing Information is disclosed to Meta, Defendant instead chose to program
7 its website so that all of its customers' Private Viewing Information is disclosed to Meta.

8 57. Before transmitting its customers' Private Viewing Information to Meta, Defendant
9 failed to notify any Plaintiff or any putative Class member that it would do so, and none of them have
10 ever consented (in writing or otherwise) to these practices.

11 58. By intentionally disclosing to Meta Plaintiff's and its other purchasers' FIDs together
12 with the specific video content they each requested or obtained, without Plaintiff's or any of its other
13 purchasers' consent to these practices, Defendant knowingly and systematically violated the VPPA
14 on an enormous scale.

15
16
17
18 **CLASS ACTION ALLEGATIONS**

19 59. Plaintiff seeks to represent a class defined as all persons in the United States who,
20 during the two years preceding the filing of this action, purchased video content from Defendant's
21 website while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

22 60. Class members are so numerous that their individual joinder herein is impracticable.
23 On information and belief, members of the Class number in at least the tens of thousands. The precise
24 number of Class members and their identities are unknown to Plaintiff at this time but may be
25 determined through discovery. Class members may be notified of the pendency of this action by mail
26 and/or publication through the membership records of Defendant.

1 61. Common questions of law and fact exist for all Class members and predominate over
2 questions affecting only individual class members. Common legal and factual questions include, but
3 are not limited to: (a) whether Defendant knowingly disclosed Plaintiff's and Class members' Private
4 Viewing Information to Meta; (b) whether Defendant's conduct violates the Video Privacy Protection
5 Act, 18 U.S.C. § 2710; (c) whether Defendant should be enjoined from disclosing Plaintiff's and
6 Class members' Private Viewing Information to Meta; and (d) whether Plaintiff and Class members
7 are entitled to statutory damages for the aforementioned violations.
8

9 62. The named Plaintiff's claims are typical of the claims of the Class in that the named
10 Plaintiff and the Class members suffered invasions of their statutorily protected right to privacy (as
11 afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be
12 highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in
13 intentionally disclosing their Private Purchase Information to Meta.
14

15 63. Plaintiff is an adequate representative of the Class because her interests do not conflict
16 with the interests of the Class members he seeks to represent, he has retained competent counsel
17 experienced in prosecuting class actions, and he intends to prosecute this action vigorously. Plaintiff
18 and her counsel will fairly and adequately protect the interests of Class members.
19

20 64. The class mechanism is superior to other available means for the fair and efficient
21 adjudication of Class members' claims. Each individual Class Member may lack the resources to
22 undergo the burden and expense of individual prosecution of the complex and extensive litigation
23 necessary to establish Defendant's liability. Individualized litigation increases the delay and expense
24 to all parties and multiplies the burden on the judicial system presented by this case's complex legal
25 and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory
26 judgments. In contrast, the class action device presents far fewer management difficulties and
27 provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a
28

1 single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure
2 that all claims and claimants are before this Court for consistent adjudication of the liability issues.

3
4 **CAUSE OF ACTION**
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

5 65. Plaintiff repeats the allegations asserted in the preceding paragraphs as if fully set forth
6 herein.

7 66. Plaintiff brings her claim individually and on behalf of the putative Class Members
8 against Defendant.

9 67. The VPPA prohibits a "video tape service provider" from knowingly disclosing
10 "personally identifying information" concerning any "consumer" to a third party without the
11 "informed, written consent (including through an electronic means using the Internet) of the
12 consumer." 18 U.S.C. § 2710.

13 68. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person,
14 engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of
15 prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape
16 service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of
17 delivering audiovisual materials that are similar to prerecorded video cassette tapes and those sales
18 affect interstate or foreign commerce.

19 69. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or
20 consumer of goods or services from a video tape service provider." As alleged above, Plaintiff and
21 Class members are consumers because they purchased prerecorded video content from Defendant's
22 website. Thus, Plaintiff and Class members are "consumers" as defined in 18 U.S.C. § 2710(a)(1).

23 70. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes
24 information which identifies a person as having requested or obtained specific video materials or
25

1 services from a video tape service provider.” Defendant knowingly disclosed Plaintiff’s and Class
2 members’ Private Viewing Information to Meta in the manner alleged herein. The Private Viewing
3 Information that Defendant transmitted to Meta constitutes “personally identifiable information” as
4 defined in 18 U.S.C. § 2710(a)(3) because the transmitted information identified Plaintiff and each
5 Class member to Meta as an individual who purchased video content, including the specific video
6 materials requested or obtained from Defendant’s website.

7
8 71. Defendant never obtained informed, written consent from Plaintiff or any Class
9 member to disclose their Private Viewing Information to Meta or any other third party. More
10 specifically, Defendant never obtained from Plaintiff or any Class member informed, written consent
11 in a form distinct and separate from any form setting forth other legal or financial obligations of the
12 consumer; Defendant never obtained from Plaintiff or any Class member informed, written consent
13 that, at the election of the consumer, was given at the time the disclosure is sought or was given in
14 advance for a set period of time, not to exceed two years or until consent is withdrawn by the
15 consumer, whichever is sooner; and Defendant never provided an opportunity, in a clear and
16 conspicuous manner, for Plaintiff or any Class member to withdraw consent on a case-by-case basis
17 or to withdraw consent from ongoing disclosures, at the consumer’s election. *See* 18 U.S.C. §
18 2710(b)(2).
19

20
21 72. Defendant knowingly disclosed such information to Meta because Defendant
22 intentionally installed and programmed the Meta Pixel code on its website, knowing that such code
23 would transmit to Meta the video titles requested by its purchasers and its purchasers’ unique
24 identifiers (including FIDs) when purchasers’ requested or obtained videos from its website.

25 73. By disclosing Plaintiff’s and Class members’ Private Viewing Information, Defendant
26 violated their statutorily protected right to privacy in the videos they requested or obtained from
27 Defendant. 18 U.S.C. § 2710(c).
28

74. As a result of these violations, Defendant is liable to Plaintiff and Class members for damages and other relief as provided by the VPPA.

75. On behalf of herself and all members of the Class, Plaintiff seeks to enjoin Defendant's future disclosures of its purchasers' Private Viewing Information; liquidated damages in the amount of \$2,500 per violation of the VPPA; reasonable attorneys' fees and costs; and all other preliminary or equitable relief the Court deems appropriate. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant KD Creatives, Inc. d/b/a Big Little Feelings as follows:

- A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- B. For an order declaring that Defendant's conduct as described herein violated the VPPA;
- C. For an order finding in favor of Plaintiff and the Class and against Defendant on all counts asserted herein;
- D. For an award of \$2,500.00 to the Plaintiff and each Class member, as provided by the VPPA, 18 U.S.C. § 2710(c);
- E. For an order permanently enjoining Defendant from disclosing the Private Viewing Information of its purchasers to third parties in violation of the VPPA.
- F. For prejudgment interest on all amounts awarded; and
- G. For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Class under Rule 23 and 18 U.S.C. § 2710(c).

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

1
2 Dated: September 12, 2024

Respectfully submitted,

3
4 /s/ Frank S. Hedin

5 **HEDIN LLP**

6 FRANK S. HEDIN

535 Mission Street, 14th Floor

7 San Francisco, CA 94105

TELEPHONE: (305) 357-2107

8 FACSIMILE: (305) 200-8801

9 FHEDIN@HEDINLLP.COM

10 *Counsel for Plaintiff and Putative Class*
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28